EUGridPMA
Status and Current Trends
and some IGTF topics

June 2014
Lehi, UT, US

David Groep, Nikhef & EUGridPMA
EUGridPMA Topics

- EUGridPMA (membership) status
- Towards an African presence in the IGTF
- Risk Assessment Team status
- IPv6 readiness and fetch-crl
- Generalised MICS profile
- Private Key Protection Guidelines v2.0
- Heartbleed
- On-line CA Architectures Guideline document
- IGTF Repositioning

See summary at https://www.eugridpma.org/meetings/2014-05/
Geographical coverage of the EUGridPMA

- 25 of 27 EU member states (all except LU, MT)
- + AM, CH, DZ, EG, HR, IL, IR, IS, IO, MA, MD, ME, MK, NO, PK, RO, RS, RU, SY, TR, UA, CERN (int), DoEGrids(US)* + TCS (EU)

Pending or in progress
- ZA, KE, TZ, SN, TN, AE, GE
Membership and other changes

- Responsiveness challenges for some members
  - JUNET CA – suspended
  - HIAST CA – keeps running (albeit with some connectivity issues)

- CA reduction and growth
  - More countries moved to TCS: IUCC IL, IE, ...
  - DoEGrids & ESnet decommissioned (as of 1.56 release)
  - TCS tender ongoing, target start of overlap period summer 2014
  - New CA in Georgia (Tblisi), many from UbuntuNet &c

- Self-audit review
  - Kaspars Krampis as dedicated review process coordinator
  - Self-audits progressing on schedule for most CAs
  - biggest challenge in getting peer reviewers to actually review
Activities in Africa

Big Science in Africa - the SKA

A Network Centric View of the SKA

- Receptors/sensors
  - ~15,000 Tbps aggregate
- Correlator / data processor
  - ~1000 km
  - 400 Tbps aggregate
- Supercomputer
  - ~25,000 km
  - (Path to London via USA)
  - ~13,000 km
  - (South Africa to London)
  - 0.1 Tbps (100 Gbps) aggregate

European distribution point

Hypothetical (based on the LHC experience)

Many similar astro activities,
- e-VLBI Africa (South Africa, Ghana)
- Namibia HESS, CTA.

Bruce Becker: Coordinator, SAGrid | bbecker@csir.co.za | http://www.sagrid.ac.za
Wide science in Africa - H3A BioNet

Genomics and environmental determinants of common diseases in order to improve health in Africa;
Full genome sequencing of various populations in Africa

32 partner institutions in 15 African countries, 2 in US
Regional NREN Alliances

- Regional NREN alliances have membership of the various NRENS
- Provide an umbrella body for new services, etc
- The natural home for CA, IdF services...
Current and upcoming CAs in Africa

In North-Africa and ASREN region already

- Morocco, Algeria, Egypt

Coming soon

- South-Africa, Kenya, Tanzania, Senegal, Ghana, Nigeria, …

With e-Infrastructure help from incubator projects like CHAIN-REDS, eI4Africa, &c
Tartu summary on an ‘African PMA’

‘This activity (and the size of the continent and number of prospective authorities and projects in Africa) in itself merits the thought of establishing a dedicated PMA for Africa in the future, with preliminary actions to that effect mirroring the developments in the Americas with a dedicated 'chapter'.’

‘There is in the PMA quite wide support for an African PMA after the activities have been 'bootstrapped' and sufficient experience built up in the region to sustain the (effort intensive) review and accreditation processes.’

‘The concept of having in the future (2 years or so) a identifiable African presence in the IGTF is supported by the EUGridPMA.’
MISCELLANEOUS TOPICS

RAT communications challenge
IPv6
Generalised MICS profile
Private Key Protection Guidelines v2.0
Heartbleed
On-line CA Architectures Guideline document
IGTF repositioning and new byline
RAT CHALLENGE
RAT challenge

- Ursula Epting to conduct early June against all CAs
- Timeline *taking into account time zones*
  - 4th June, Announcement of the test
  - 18th June, 10.20 h, Start of the test
  - 20th June, 14.50 h, Reminder for not replying CA's
  - 21th June, 10.20 h, End of the test

- Request for
  - Acknowledge receipt
  - for each trust anchor
Results (2)

Furthermore 4 CA's replied later, after the official deadline. 

So in the very end 13 % did not reply at all. 

This comes down to 11 CA's (with 'one CA' as 'one structure')
Results

IGTF-rechallenge February 2014

Notice: automatic replies of e.g. ticket systems were not counted
Interpretation of the results

In a strict interpretation we can say that only 36 % fullfilled the requirement to react within one business day – while 74 % failed.

(Results communication test 2013: 76 % fullfilled the requirement - 24 % failed.

In a softer interpretation we can say that 57 % are responsive while 43 % are not.
<table>
<thead>
<tr>
<th>Rechallenge February 2014</th>
<th>Date</th>
<th>Mail Address from IGTF release</th>
<th>Mail sent 11.11h a.m.</th>
<th>Message received until</th>
<th>Reminder bday 2</th>
<th>Weekend</th>
<th>Reminder bday 3</th>
<th>Reminder bday 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>APAC</strong></td>
<td>26th Feb</td>
<td><a href="mailto:camanager@vpac.org">camanager@vpac.org</a></td>
<td>x</td>
<td>12.11, 13.11, 10.11</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CNRS2/CNRS2-Grid-FR/CNRS2-Projets</strong></td>
<td>26th Feb</td>
<td><a href="mailto:grid.fr@renater.fr">grid.fr@renater.fr</a></td>
<td>x</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>EG-GRID</strong></td>
<td>26th Feb</td>
<td><a href="mailto:ca@grid.eu.nl">ca@grid.eu.nl</a></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>HIAST</strong></td>
<td>26th Feb</td>
<td><a href="mailto:cagrd@hiast.edu.sys">cagrd@hiast.edu.sys</a></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>IGCA</strong></td>
<td>26th Feb</td>
<td><a href="mailto:igca@edac.in">igca@edac.in</a></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>IHEP/IHEP-2013</strong></td>
<td>26th Feb</td>
<td><a href="mailto:gridca@ihep.ac.cn">gridca@ihep.ac.cn</a></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td><strong>IRAN-GRID</strong></td>
<td>26th Feb</td>
<td><a href="mailto:ca-marager@ipm.ir">ca-marager@ipm.ir</a></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>JUnet-CA</strong></td>
<td>26th Feb</td>
<td>suspended</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NCHC</strong></td>
<td>26th Feb</td>
<td><a href="mailto:nchcc@nchc.org.tw">nchcc@nchc.org.tw</a></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NECTEC</strong></td>
<td>26th Feb</td>
<td><a href="mailto:camanager@hpcc.nectec.or.th">camanager@hpcc.nectec.or.th</a></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td><strong>UniandesCA</strong></td>
<td>26th Feb</td>
<td><a href="mailto:ca@uniandes.edu.co">ca@uniandes.edu.co</a></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>BYCCA</strong></td>
<td>26th Feb</td>
<td><a href="mailto:ca@newman.bas.net.by">ca@newman.bas.net.by</a></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NERSC-SLCS</strong></td>
<td>26th Feb</td>
<td><a href="mailto:certs@nersc.gov">certs@nersc.gov</a></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>PolishGrid</strong></td>
<td>26th Feb</td>
<td><a href="mailto:pigrid-ca@man.poznan.pl">pigrid-ca@man.poznan.pl</a></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td><strong>UNLPGrid</strong></td>
<td>26th Feb</td>
<td><a href="mailto:ca@pkigrid.unlp.edu.ar">ca@pkigrid.unlp.edu.ar</a></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

**Meaning of Colours**
- Light green = good
- Dark green = replied but too late
- Brown = replied but much too late
- Red = didn't reply at all
- Light blue = not tested
- Blue = results/info
Suggestion for improvement

● The CA's not replying at all to the test should be contacted by their PMA-chairs.

● An explanation about the failing should be provided to IGTF-RAT team.

● The reasons for failing should be eliminated.

~~~~~~~~~~~~

● The communication test should be repeated - for all CA's – at the end of this year, so we get used to having a challenge once a year.
IPV6
IPv6 status

- FZU runs a continuous v6 CRL monitor
  http://www.particle.cz/farm/admin/IPv6EuGridPMACrlChecker/

- 23 CAs offer working v6 CRL
  - but there are also 4 CAs that give an AAAA record but where the GET fails …
  - Still 71 endpoints to go (but they go in bulk)
  - dist.eugridpma.info can act as v6 source-of-last-resort

- fetch-crlv3 v3.0.10+ has an explicit mode to force-enable IPv6 also for older perl versions
  - Added option "--inet6glue" and "inet6glue" config setting to load the Net::INET6Glue perl module (if it is available) to use IPv6 connections in LWP to download CRLs
<table>
<thead>
<tr>
<th>Certificate Authority</th>
<th>O</th>
<th>C</th>
<th>Result</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEK GRID Certificate Authority</td>
<td>CRC</td>
<td>JP</td>
<td>YES</td>
<td><a href="http://gridca.kek.jp/repository/617ff41b.r0">http://gridca.kek.jp/repository/617ff41b.r0</a></td>
</tr>
<tr>
<td>KISTI Grid Certificate Authority</td>
<td>GRID</td>
<td>KR</td>
<td>NO</td>
<td><a href="http://ca.gridcenter.or.kr/CRL/722e5071.crl">http://ca.gridcenter.or.kr/CRL/722e5071.crl</a></td>
</tr>
<tr>
<td>UFF Latin American and Caribbean Catch-all Grid CA</td>
<td>UFF</td>
<td>BR</td>
<td>NO</td>
<td><a href="http://lacgridca.ic.uff.br/crl/cacrl.crl">http://lacgridca.ic.uff.br/crl/cacrl.crl</a></td>
</tr>
<tr>
<td>LIP Certification Authority</td>
<td>LIPCA</td>
<td>PT</td>
<td>NO</td>
<td><a href="http://ca.lip.pt/lip-lisboa/pub/crl/cacrl.pem">http://ca.lip.pt/lip-lisboa/pub/crl/cacrl.pem</a></td>
</tr>
<tr>
<td>MaGrid CA</td>
<td>MaGrid</td>
<td>MA</td>
<td>NO</td>
<td><a href="http://ra.magrid.ma/pub/crl/cacrl.pem">http://ra.magrid.ma/pub/crl/cacrl.pem</a></td>
</tr>
<tr>
<td>MARGI-CA</td>
<td>MARGI</td>
<td>MK</td>
<td>ERR</td>
<td><a href="http://www.margi.marnet.net.mk/CA/margi-v2.crl">http://www.margi.marnet.net.mk/CA/margi-v2.crl</a></td>
</tr>
<tr>
<td>MD-Grid CA</td>
<td>Certification Authority</td>
<td>RENAM</td>
<td>MD</td>
<td>NO</td>
</tr>
<tr>
<td>MREN-CA</td>
<td>MREN</td>
<td>ac, me</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td>NAREGI CA</td>
<td>CGRD</td>
<td>JP</td>
<td>YES</td>
<td><a href="http://www.naregi.org/ca/out-CRL2.crl">http://www.naregi.org/ca/out-CRL2.crl</a></td>
</tr>
<tr>
<td>NCHC CA</td>
<td>NCHC</td>
<td>ORG</td>
<td>YES</td>
<td><a href="http://ca.goc.nchc.org.tw/nchccca/CRL/NCHCCRL.der">http://ca.goc.nchc.org.tw/nchccca/CRL/NCHCCRL.der</a></td>
</tr>
<tr>
<td>GridShib CA</td>
<td>Certificate Authorities</td>
<td>National Center for Supercomputing</td>
<td>NO</td>
<td></td>
</tr>
</tbody>
</table>
On-line CA architecture - guidelines

EUGridPMA will (finally) draft the "On line CA Guidelines"

- based on current wording in the Classic profile
- keep the network separation (models A or B, where A with a private link between RA and signing system preferred)
- Allow import of a key pair into a token (taking it out of FIPS L3 mode) as long as there is a well-documented key generation and import ceremony
- L2 HSMs allowed if compensatory controls are in place
  Keeping tokens and their systems in a solid safe-box and in a closed and locked cabinet in a monitored machine room is considered adequate
- Keys are permanently activated anyway, so L3 mode (separate usage functions like generation or use) is not used for our purposes
- Activation on boot should be manual (so the operator must be required to be present)
Generalized MICS profile?

In line with the new IGTF byline, it would be beneficial to 'generalise' the current MICS profile and turn it into a pure LoA document describing the requirements on identity authorities (IdPs or CAs) given needs of the relying parties and SPs. Since the MICS is the closest one to the current federation model, it is the appropriate starting place.

Unfortunately, the PMA meeting at this point ran out of time, so the details are deferred to the next meeting. In particular, we would like to ask the TAGPMA (the 'hosts' of the MICS profile) to consider this discussion for the next TAGPMA meeting in Lehi. The generalisation would imply:
- removal of the PKI specific bits of the text
- recast it as a 'Level of identity Assurance' text, representing the coordinated (harmonized) consensus of the relying party expectations and requirements
- be complementary (and not overlap with) the SCI requirements

This will then complement the (lower) IOTA level, which is already almost technology-agnostic.
Private Key Protection Life Cycle

- The (last) final changes were made to the private key protection guidelines document

http://wiki.eugridpma.org/Main/PrivateKeyProtectionLifeCycle

- It supports all the use cases currently permitted under the PKP guidelines version 1.1, but it is better reflecting the key life cycles and clarifies the roles of the participants.
Heartbleed

- Surprisingly **few revocations**! Why??
- The operational readiness of the CAs was increased once the vulnerability was known and the RPs were happy with the quick service received.
- The OpenSSL disclosure process has improved
In the future …

- quiet consensus that the authorities are willing to work operationally with the CSIRT teams to get issues resolved quickly (the IGTF typically sees a 'different side' of the issue, and has other ways to contact the subscribers)
- sharing testing tools proactively on the mailing lists is encouraged.
- These will not be publicly shared but remain within the IGTF trust circle.
- We will use the Wiki (PMA member access only!) to share such tools and restricted information
- the IGTF can also scan itself – some infrastructures (EUDAT) may never have scanner from the RP side
- message templates for subscribers can also be shared (again on the Wiki)
On-line CA Architecture Doc

- The on-line CA guidelines document was not discussed due to lack of time, but everyone is encouraged to review the draft available at

  https://wiki.eugridpma.org/Main/GuidelinesForOnLineCAs

- If access to the Wiki is not possible, please send your DN to the EUGridPMA operations folk (info@eugridpma.org) to get your account activated on the Wiki. Read-only access (through plain http) is open to the whole world.
IGTF REPOSITIONING
Attributes and authorization becoming more important

- mere identity authentication is likely to become commonplace in the years to come (academic federations, commercial ID providers, etc.)

- But authorization, (community) assured attributes, and attribute composition are unsolved for research: the IGTF can reposition itself to address these new challenges

- anyway consolidation of federations in the research and academic space means that there need be less emphasis on the classical CA work
Already ongoing ...

- AA Operations Guideline
- Guideline on Trusted Credential Stores
- IOTA as a basis for community-provided assurance
Beyond the current framing: IGTF as a brand, not an acronym

Proposal

- IGTF be no longer considered an acronym, but be treated as a word where we can associate it with a more appropriate byline.
- Based on an extensive discussion by those present, it was concluded that a proposal be circulated to the other PMAs with a new 'byline':

**IGTF: Interoperable Global Trust Federation**

supporting distributed IT infrastructures for research
A new motto and mission ...

"The IGTF -through its members- develops guidance, coordinates requirements, and harmonizes assurance levels, for the purpose for supporting trust between distributed IT infrastructures for research.

This goal is accomplished by the members of the IGTF through coordination of providers of trust information (authorities) and consumers thereof (relying parties) and by adoption of common standards, minimum requirements, and best practices for policy, technical security, and operational trust."

Needs a revised charter - draft done in EUGridPMA, can we converge here this week?
https://wiki.eugridpma.org/Members/IGTFFederationDocument
If you concur ...

- Update IGTF Federation Document (Charter)
- Revise IGTF logo and web site – done

- Encourage wider participation in the IGTF, in particular by relying parties and infrastructures, with an emphasis on those having operational (security) aspects and/or representing relying user communities
  - role to play for 'catch-all' cases as well? – many of the current organisations and authorities also work 'bottom-up' serving limited numbers of researchers across a large number of institutions (with a few people each) – this is not traditional use case for Refederations … but it is for commercial IdPs
IGTF Web Site

Ongoing, some changes already done. Proposed

- public-facing (RP, general public) function should be separated from any internal use
  - primary audience is RPs and 'general' public
  - it should include a section for 'our own' integral IGTF use with links, agenda, &c

- add an introduction for 'humans'
  - links to interviews and (iSGTW-like) articles about IGTF
    everyone to send these to <webmaster@igtf.net>
  - add a 'news' box with current information (to change monthly or so).

- Make map more prominent
  - The mini-map should link to a PMA page with a click-able map or membership list
  - encourage TAGPMA and APGridPMA to maintain a list of their meeting that can be linked to
REVIEW THE DRAFT CHARTER THIS WEEK …
UPCOMING MEETINGS
EUGridPMA Agenda

- 32nd PMA meeting
  8-10 September 2014 (Poznan, PL)

- 33rd PMA meeting
  12-14 January 2015, Berlin, DE (offered by DFN)